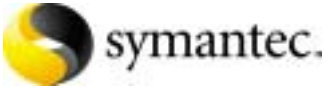
ManHunt™ Smart Agent for NetScreen®

Installation Guide



ManHunt Smart Agent for Netscreen Installation Guide

Copyright Notice

Trademarks

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC SOFTWARE LICENSE AGREEMENT (Smart Agent)

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. License.

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to you. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

A. use that number of copies of the Software as have been licensed to you by Symantec under a License Module for Your internal business purposes. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, you may make one copy of the Software you are authorized to use on a single machine.

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of your computer and retain the original for archival purposes;

C. use each licensed copy of the Software on a single central processing unit; and

D. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this license.

You may not:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless you have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module; nor

F. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content

Updates"). You may obtain Content Updates for any period for which you have purchased upgrade insurance for the product, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. Export Regulation:

Export, re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England.

This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

ManHunt Smart Agent for NetScreen®

The ManHunt Smart Agent (MSA) for NetScreen® enables ManHunt to receive events in real time from a NetScreen appliance, convert these events into the ManHunt event format, and then send the events to a ManHunt node for aggregation and correlation with all other ManHunt events. The MSA also enables you to set response policies for NetScreen events in the ManHunt Policy Configuration interface. (Refer to the ManHunt Administration Guide for instructions on creating response policies.)

Note: The MSA for NetScreen sends only malicious activity and attack events (intrusion detection events) received from a NetScreen appliance to the ManHunt node.

To use the MSA for NetScreen, perform the following steps.

1. Ensure you have installed ManHunt 2.11 or later.
2. Verify that the NetScreen appliance is running ScreenOS 3.0.2 or later. The MSA will work with all NetScreen appliances (from NetScreen 5XP through NetScreen 5000).
3. Configure NetScreen.
   See "Configuring NetScreen" on page 2.
4. Install the MSA for NetScreen.
   See "Installing the MSA for NetScreen" on page 2.
5. Install the NetScreen meta data on the ManHunt node.
   See "Installing the NetScreen Meta Data" on page 3.
6. Configure ManHunt to receive events from the MSA for NetScreen.
   See "Configuring ManHunt" on page 4.

7 Start the MSA for NetScreen.
See “Starting and Stopping the MSA” on page 8.

Configuring NetScreen

Use the NetScreen web interface to configure the NetScreen appliance to send SNMP traps to the IP address of the MSA host. (See the NetScreen documentation for more information.)

To configure the NetScreen appliance to send SNMP traps

1 Click System > Admin in the left frame of the NetScreen console.

2 Click SNMP in the right frame and specify the SNMP ports the appliance will use.

3 Click New Community at the bottom of the frame.

4 Enter the Community Name in the right frame.

5 Check Trap in Permissions for MSA NetScreen to work correctly.

Note: The other permissions are optional; using them will increase the load on the MSA host.

---

6 Type in the IP addresses of the MSA hosts to which the NetScreen appliance will send alerts via SNMP traps.

Installing the MSA for NetScreen

The MSA for NetScreen must be installed on a host running Solaris 8 on SPARC or Intel®. You can deploy the MSA for NetScreen in either of two deployment modes:

- Install the MSA on the ManHunt node.
- Install the MSA on a dedicated host.

Note: The MSA can not be installed on the NetScreen appliance.

In either deployment, the MSA listens for NetScreen SNMP traps on port 162 by default. The MSA converts the SNMP traps into the ManHunt event format, and sends the events to ManHunt over EDP (Event Dispatch Protocol). EDP communication between ManHunt and the MSA is secure and encrypted.

You must be logged in as root to run the install script.

To install the MSA for NetScreen

1. Place the CD in the CD-ROM drive; mount the drive if necessary.
2. Change to the CDROM directory and enter:

   ```
   ./install.sh
   ```

3. Enter a directory where you want to install the MSA or accept the default directory **`/usr/msanetscreen`**. Press Enter.
4. Enter a directory to which the MSA will write log files or accept the default **`<MSA_install_dir>/logs`**. Press Enter.
5. Enter the IP address of the ManHunt node that will accept the NetScreen event data. Press Enter.
6. Enter the EDP port number used by this ManHunt node. By default, the ManHunt installation process sets this port to 1333. If you have not edited this port number for the ManHunt node, accept the default port 1333. Press Enter.
7. Enter the EDP passphrase. Press Enter.

Note: This is identical to the passphrase you enter when you create the external sensor node for the MSA for NetScreen.

See "Changing the EDP Passphrase" on page 7.

---

8. Re-enter the EDP passphrase. Press Enter.

Installing the NetScreen Meta Data

You must install the NetScreen meta data on the ManHunt node you log into from the administration console, typically the primary master node. This is done in order for you to be able to create the MSA for NetScreen external sensor node; create response policies for NetScreen events; and display NetScreen event data in the ManHunt administration console.

In addition, you must install this meta data on the ManHunt node that will receive the NetScreen event data from the MSA for NetScreen (if different from the master node).

You must be logged in as root to install the NetScreen meta data.

To install the NetScreen meta data

1. Place the CD in the CD-ROM drive; mount the drive if necessary.
2. Change to the CDROM directory and enter:

```
./install-md.sh
```

3 Ensure the meta data file to be installed begins with 'netscreen'. If so, press Enter when prompted to continue with the installation.

Allow the installation process to complete and allow the installer to restart ManHunt. If this is the ManHunt node used for administration, quit and restart any administration consoles connected to the node to enable the consoles to incorporate the new meta data.

Configuring ManHunt

To enable communication between ManHunt and the MSA for NetScreen and to be able to set ManHunt response policies for NetScreen events, you must create an external sensor node in the ManHunt topology tree for the machine on which the MSA for NetScreen is installed.

To add an external sensor node

1 Open the ManHunt administration console.

2 Right-click External Sensors in the topology tree and click Add External Sensor in the pop-up menu.

3 In Add External Sensor enter a name of up to 39 characters for the device. This name will appear in the topology tree.

4 Enter a customer ID.

5 Enter the IP address for the machine on which you installed the MSA for NetScreen.

6 Click NetScreen in Smart Agent Type.

Note: The NetScreen Smart Agent type only appears in the drop-down list if you have installed the NetScreen meta data.

---

7 Select the ManHunt node that will receive event data from the MSA for NetScreen.

Note: You must select the ManHunt node before setting the EDP passphrase. ManHunt sets the EDP passphrase for the ManHunt node that is selected in the Event Receiver box at the time that you enter the EDP passphrase.

---

8 Set the EDP passphrase. This passphrase was also entered during step 6 of the MSA for NetScreen installation process.

9 Enter a description for the MSA for NetScreen. This description will be displayed on the main console screen when this external sensor node is selected in the topology tree.

10 Click OK, then click Save Changes to save your topology tree changes.

Configuring the MSA for NetScreen

The MSA installation process creates a configuration file called `netscreen2mh.conf` in the `<MSA_install_dir>/etc` directory. This file contains parameters for MSA operation and for connecting to the ManHunt node. These parameters are described in Table 1-1.

MSA Configuration File

The configuration file is broken down into sections with section headers enclosed in brackets `[]`. The first section is called [MSA] and contains most of the configuration parameters. The second section is called [SNMP]. The following is a sample configuration file:

```
[MSA]
    ManHuntHostIPAddr = 10.0.0.34:1333
    EDPSecret = DokdYjNU732mnDuj
    MSALogDir = /usr/msanetscreen/logs
    MSALogLevel = 5
    EventDefinitionFile = /usr/msanetscreen/etc/netscreen2mh.evtdef
[SNMP]
```

Note: Table 1-1 lists all editable parameters. If you edit any of the configuration parameter values, you must restart the MSA application. See "Starting and Stopping the MSA" on page 8.

Table 1-1 MSA Configuration File Parameters

Parameter	Description
`ManHuntHostIPAddr`	The IP address of the ManHunt node to which the NetScreen events are sent. The format is `IP address:port`. The port must be the port on which ManHunt is configured to receive events. The default port is 1333. If you change the EDP Port Number parameter on the ManHunt node, be sure to change the value in the MSA configuration file to match, and vice versa. This parameter is required.
`EDPSecret`	The value for `EDPSECRET` is the encrypted form of the EDP passphrase and is set during MSA installation. Do not attempt to edit this parameter from within the configuration file. This parameter is required.
`EventDefinitionFile`	Path to the event definition file. The MSA conversion engine uses instructions contained in the event definition file to convert NetScreen alerts into ManHunt events. This parameter is required.
`MSALogDir`	The directory to which the MSA should write its log file. The default value is `<MSA_install_dir>/msanetscreen/logs`. If you delete this parameter from the configuration file, then the default log directory becomes `/tmp`.
`MSALogLevel`	An integer specifying the level of logging that the MSA uses. Possible values are from 1 to 35 with 35 being the most verbose. The default value is 5. If you raise the log level above 5, the log files may become large enough to negatively impact MSA performance. This parameter is optional.

Table 1-1 MSA Configuration File Parameters

Parameter	Description
`EventSendRate`	An integer specifying the maximum number of events per second that can be passed to the ManHunt node. If this parameter is not specified in the configuration file, the default value is 10 events per second. If you add this parameter, place it in the `[MSA]` section.
`MaxEventsinCache`	An integer specifying the maximum number of events allowed in the cache before the oldest event is dropped. If this parameter is not specified in the configuration file, the default value is 3000. If you add this parameter, place it in the `[MSA]` section.
`SnmpTrapPort`	An optional argument that allows SNMP traps to be collected on a port other than the default, which is port 162.

Changing the EDP Passphrase

To change the EDP passphrase on the ManHunt node, edit the external sensor topology tree node. The EDP passphrase on the ManHunt node must match the EDP passphrase on the MSA for NetScreen machine. Therefore, if you change the passphrase on the ManHunt node, you must also change the passphrase on the MSA for NetScreen machine by running the `changesecret` command located in the `<MSA_install_directory>/bin` directory.

To change the EDP passphrase on the ManHunt node

1. Log into the ManHunt administration console.
2. Right-click the appropriate ManHunt node and click Edit Device in the popup menu.
3. In Edit External Sensor click Set Passphrase.
4. In Change Passphrase enter the new passphrase the ManHunt node will use to communicate with the MSA for NetScreen. The passphrase must be at least 8 characters long.
5. Re-enter the passphrase for confirmation.
6. Click OK.
7. Click OK in the Edit External Sensor dialog.
8. Go to the Edit Topology menu and click Save Changes.

To change the EDP passphrase on the MSA for NetScreen machine

1. Go to the `<MSA_install_dir>/bin` directory.
2. Enter the following command:

   `./changesecret <MSA_install_dir>/etc/netscreen2mh.conf`
3. Enter the old passphrase.
4. Enter the new passphrase. The passphrase must be at least 8 characters long.
5. Re-enter the new passphrase.
6. Restart the MSA application. See "Starting and Stopping the MSA" on page 8.

Note: If you have forgotten the old passphrase, you can delete the EDPSecret line from the configuration file `<MSA_install_dir>/etc/netscreen2mh.conf` and then run `changesecret` again. The script will not prompt for the old passphrase once the passphrase line is removed. See "Configuring the MSA for NetScreen" on page 5.

Starting and Stopping the MSA

The MSA installer creates startup scripts in the system startup directories `/etc/init.d` and `/etc/rc2.d` to automatically start the MSA for NetScreen when the machine is rebooted. In addition, start and stop scripts are provided in the `<MSA_install_dir>`. You must be logged in as root to run these scripts. They are installed in the root MSA install directory. Simply run `start` or `stop` to start or stop the MSA.

Uninstalling the MSA

To uninstall the MSA, go to the `<MSA_install_directory>/install` directory and run the `uninstall` script.